Oversight Hearing

"No Computer System Left Behind: A Review of the Federal Government's D+ Information Security Grade"

Thursday, April 7, 2005
10:00 a.m.
Room 2154 Rayburn House Office Building

Opening Statement

Good morning. A quorum being present, the Committee on Government Reform will come to order. I would like to welcome everyone to today's hearing on the implementation of FISMA, the Federal Information Security Management Act of 2002.

We rely heavily on information technology and the Internet to support our economy, national security, and government operations. For instance, e-commerce is more popular than ever – Christmas 2004 saw record high consumer demand on retail websites. IT systems are used to operate and protect our critical infrastructures. And in the federal government, electronic government initiatives create efficiencies, save taxpayers time and money, and help eliminate redundant processes.

Given the interconnectivity of systems, all it takes is one weak link to break the chain. All users – whether they are at home, school, or work – need to understand the impact of weak security and the measures that should be taken to prevent or respond to cyber attacks.

Everyone must protect his or her piece of cyberspace – that includes the government. Therefore, it is critical that the federal government adequately protect its systems to ensure the continuity of operations and to maintain public trust. This is particularly true of agencies such as the Internal Revenue Service, the Social Security Administration, and the Department of Veterans Affairs that maintain citizens' personal information in their systems. Recent failures have focused the spotlight on identity theft. Successful FISMA implementation is important because a similar event could occur in the government. Like the private sector, agencies are not immune to the loss of personal

information. Threats to government systems could result in identity theft and subsequent financial damage and frustration, as well as diminished trust in government IT capabilities and electronic government programs.

Everyday, federal information systems are subjected to probes or attacks from outside sources. Cyber attacks are evolving and becoming more sophisticated. Therefore, a government information security management program must be comprehensive, yet flexible enough to adapt to the changing cyber threat environment. It is a matter of good management and good business practice, but it's also a matter of national security. FISMA provides that structure, by requiring each agency to create a comprehensive risk-based approach to agency-wide information security management.

OMB performs an important role in the information security management process by encouraging agencies to adopt a new approach to security. In the past, information security was often seen as an afterthought – more of a crisis response than a management tool. OMB is helping to alter that perspective. It holds the agencies responsible for protecting federal systems through business case evaluations so that agencies can better fulfill their missions. OMB requires agencies to address their security deficiencies before they are permitted to spend money on IT upgrades or new IT projects. I support this action because it forces agencies to concentrate on security before adding new layers of systems to their architecture and potentially complicating their security concerns.

I am also pleased that OMB has identified a sixth line of business – cyber security. Laws like FISMA and the Clinger-Cohen amendment require every agency to think about and invest in information security. However, each agency does it differently. The recent FISMA grades show the Federal government still has a long way to go when it comes to information security. As with the other five lines of business, the goal of the cyber security line of business is to use business principles and best practices to identify common solutions for business processes and/or technology-based shared services for government agencies. The intended result is better, more efficient and consistent security

across the Federal government for the same amount of dollars, if not less. At the end of the day, it's not how much money you spend, but how well you spend it.

To help us gauge the agencies information security progress, FISMA requires the CIOs and IGs to submit reports to Congress and OMB. The committee enlists GAO's technical assistance to prepare the annual scorecard. This year the government made a slight improvement, receiving a D+. The overall government score is two points above last year. Needless to say, this is not impressive. Progress is slow. Our objective today is to find out how the government can improve and why some agencies can show remarkable improvement while others appear to flounder.

We will hear from the IGs and CIOs of two agencies that improved their scores this year – the Department of Transportation and the US Agency for International Development. We will also hear from the IG and CIO at the Department of Homeland Security – a poor performer again this year. I think it is worth noting that DHS has cyber security responsibilities for the nation and must work with the private sector regularly on these issues. Given this role, DHS must have its house in order and should become a security leader among agencies. What's holding them up? The DHS witnesses will discuss the unique challenges they face in a large and relatively new agency, and what actions they are taking to improve their information security.

In addition, we are concerned about how well the CIO and IG offices communicate about issues such as their interpretations of the OMB reporting requirements. Disagreements on interpretation may impact their respective reports and make it difficult for us to get an accurate picture of the agency's information security progress. This also raises questions about the clarity of the guidance and whether agencies respond to OMB about the guidance during the comment period so their comments and concerns may be addressed in the final version.

We will examine whether the IGs need a standardized information security audit framework similar to that used for financial management systems. Also we will address

whether agencies need additional guidance, procedures, or resources to improve their information security and fully comply with FISMA.

Panel One witnesses from GAO and OMB will focus on information security from the government-wide perspective. Panel Two is comprised of agency representatives and will focus on the agency-level perspective on implementation of FISMA. We'll hear from the IGs and CIOs at USAID, DHS, and the Department of Transportation. GAO will join Panel Two for the question and answer period.